UNITED STATES PATENT AND TRADEMARK OFFICE MN

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/727,430	12/04/2003	Mark L. Buer	2875.0240001	6875

26111 7590 05/15/2007
STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
POWERS, WILLIAM S	
ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
05/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/727,430	BUER ET AL.	
	Examiner	Art Unit	
	William S. Powers	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-57* is/are pending in the application.

4a) Of the above claim(s) *34-39* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33 and 40-57* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☒ Claim(s) *34-39* are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *1/23/2006*.
4) ☒ Interview Summary (PTO-413) Paper No(s)/Mail Date. *20070502*.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. Claims 1-33 and 40-57, drawn to processing TCP data packets, classified in class 713, subclass 153.

II. Claims 34-39, drawn to configuration of processors, classified in class 709, subclass 222.

The inventions are distinct, each from the other because of the following reasons:

2. Inventions I and II are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct if they do not overlap in scope and are not obvious variants, and if it is shown that at least one subcombination is separately usable.

3. In the instant case, subcombination I has separate utility such as processing TCP packets.

4. In the instants case, subcombination II has separate utility such as configuring a hardware processor.

See MPEP § 806.05(d).

5. The examiner has required restriction between subcombinations usable together. Where applicant elects a subcombination and claims thereto are subsequently found allowable, any claim(s) depending from or otherwise requiring all the limitations of the

allowable subcombination will be examined for patentability in accordance with 37 CFR 1.104. See MPEP § 821.04(a). Applicant is advised that if any claim presented in a continuation or divisional application is anticipated by, or includes all the limitations of, a claim that is allowable in the present application, such claim may be subject to provisional statutory and/or nonstatutory double patenting rejections over the claims of the instant application.

6. During a telephone conversation with Michael Specht on May 3, 2007 a provisional election was made with traverse to prosecute the invention of Group I, claims 1-33 and 40-57. Affirmation of this election must be made by applicant in replying to this Office action. Claims 34-39 are withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Information Disclosure Statement

7. The Information Disclosure Statement submitted on 1/23/2006 has been considered.

Claim Objections

8. Claims 8, 14, 16 and 47 are objected to because of the following informality:

a. As to claims 8 and 16, using the acronym "MAC" in line 2 of the claim without specifying in the claim language what it stands for creates confusion. For

the purpose of examination, the Examiner assumes that MAC stands for Media Access Controller.

b. As to claim 14, the verbs "retrieves" in line 9, and "encrypts, decrypts and authenticates" in line 12 are not in the correct tense.

c. As to claim 47, the word "one" is missing from the phrase "at least network" in line 2 of the claim.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 1-10, 12-15, 21-23, 25, 26, 28-33, 41-48 and 54-57 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent No. 7,162,630 to Sperry et al. (hereinafter Sperry).

As to claims 1 and 57, Sperry teaches:

a. Receiving, by a security processor, packets (inbound packets (Sperry, column 9, line 4)) from a Gigabit Ethernet network (Sperry, column 5, lines 14-18).

b. Processing at least a portion of the received packets, the processing consisting of at least one of the group of encrypting, decrypting and authenticating (security arrangement has the capability of encryption, decryption and/or authentication of received data) (Sperry, column 4, lines (51-67).

c. Transmitting, from the security processor, at least one result of the processing of the at least a portion of the received packets (security arrangement has the capability of encryption, decryption and/or authentication of transmitted data) (Sperry, column 4, lines (51-67).

As to claim 2, Sperry teaches processing comprises performing IPSec operations (security processing is conformant to IPSec) (Sperry, column 5, lines 30-34).

As to claim 3, Sperry teaches the IPSec operations comprise adding or removing protocol elements (security is added to packets that have security associations that require the packet to have security protocols) (Sperry, column 14, line 64-column 15, line 2).

As to claim 4, Sperry teaches a at least a portion of the received packets comprise security association information for use in encrypting, decrypting or

authenticating the at least a portion of the received packets (the Security Protocol Index (SPI) of an inbound packet is used to access the Protocol Control Block and the Security Association of the packet, if one exists) (Sperry, column 9, lines 4-20).

As to claim 5, Sperry teaches retrieving security association information from at least one data memory (accessing security association data in order to properly handle data packets (Sperry, column 12, line 65-column 13, line 15)), wherein processing comprises encrypting, decrypting or authenticating the at least a portion of the received packets using the security association information (security arrangement has the capability of encryption, decryption and/or authentication of received data) (Sperry, column 4, lines (51-67).

As to claim 6, Sperry teaches the at least a portion of the received packets comprise at least one reference to an address of a security association, the method comprising the step of retrieving security association information from at least one data memory according to the address (security association pointers are extracted to find the appropriate security association for that packet) (Sperry, column 8, line 66-column 9, line 3), wherein processing comprises encrypting, decrypting or authenticating the at least a portion of the received packets using the security association information (security arrangement has the capability of encryption, decryption and/or authentication of received data) (Sperry, column 4, lines (51-67).

As to claims 7 and 15, Sperry teaches the security processor comprises an integrated circuit (Sperry, column 6, lines 35-37).

As to claims 8 and 42, Sperry teaches:

a. At least one Gigabit MAC (Sperry, column 8, lines 25-32).

b. At least one processor, connected to send data to and receive data from the at least one Gigabit MAC, for encrypting, decrypting or authenticating at least a portion of the data (the use of Network Protocol Processors (NPP) and Embedded Processors (EP) to transmit data, as well as perform security related tasks) (Sperry, column 8, lines 6-24).

As to claims 9 and 43, Sperry teaches the at least processor comprises at least one IPSec processor (the IPSec processing tasks are handled by the NPPs) (Sperry, column 9, lines 41-45).

As to claims 10 and 44, Sperry teaches the IPSec processor adds IPSec protocol elements to or removes IPSec protocol elements form the data (ESP encapsulation is performed by the NPPs) (Sperry, column 9, lines 41-45).

As to claims 12 and 45, Sperry teaches at least one data memory for storing security association information for use by the at least one processor (accessing

security association data in order to properly handle data packets) (Sperry, column 12, line 65-column 13, line 15).

As to claim 13, Sperry teaches at least one processor that extracts security association information from data received from the at least one Gigabit MAC and that sends the security association information to the at least one processor (accessing security association data in order to properly handle data packets) (Sperry, column 12, line 65-column 13, line 15).

As to claim 14, Sperry teaches:

a. Extracting at least one address of at least one security association for data received from the at least one Gigabit MAC (security association pointers are extracted to find the appropriate security association for that packet) (Sperry, column 8, line 66-column 9, line 3).

b. Sending the at least one address to the at least one processor (security association pointers are extracted to find the appropriate security association for that packet by the NPPs) (Sperry, column 8, line 47-column 9, line 3).

c. Retrieving security association information from a data memory according to the at least one address (obtaining security association data from the database) (Sperry, column 8, line 66-column 9, line 3).

d. Encrypting, decrypting or authenticating packets using the security association information (security arrangement has the capability of encryption,

decryption and/or authentication of received data) (Sperry, column 4, lines 51-67).

As to claim 21, Sperry teaches:

a. At least one media access controller (Sperry, column 8, lines 25-32).

b. At least one security processor (the use of Network Protocol Processors (NPP) and Embedded Processors (EP) to transmit data, as well as perform security related tasks) (Sperry, column 8, lines 6-24).

c. At least one switch for distributing or collecting packets between the at least one media access controller and the at least one security processor (the use of switches in the target environment) (Sperry, column 7, lines 5-19).

As to claim 22, Sperry teaches the at least one media access controller comprises at least one Gigabit MAC (Sperry, column 8, lines 25-32).

As to claim 23, Sperry teaches at least one processor for allocating memory space associated with security associations used by the at least one security processor (IPSec logic creates a security association and places the SA in the security policy database) (Sperry, column 11, line 61-column 12, line 3).

As to claim 25, Sperry teaches the at least one media access controller sends packets comprising security association information (Sperry, column 9, lines 4-20) to the at least one security processor (Sperry, column 8, lines 7-55 and figure 3).

As to claim 26, Sperry teaches:

a. The at least one media access controller sends packets comprising at least one address of at least one security association (security association pointers are extracted to find the appropriate security association for that packet) (Sperry, column 8, line 66-column 9, line 3) to the at least one security processor (Sperry, column 8, lines 7-55 and figure 3).

b. The at least one security processor retrieves security association information from a data memory according to the at least one address and encrypts or authenticates packets using the security association information (security arrangement has the capability of encryption, decryption and/or authentication of received data) (Sperry, column 4, lines (51-67).

As to claim 28, Sperry teaches:

a. At least one media access controller (Sperry, column 8, lines 25-32).

b. Executing TCP operations (TCP tasks are handled by the MAC) (Sperry, column 5, lines 14-42).

c. Generating information associated with at least one security association (Security Association pointers are extracted to find the appropriate security association for that packet) (Sperry, column 8, line 66-column 9, line 3).

d. At least one security processor (the use of Network Protocol Processors (NPP) and Embedded Processors (EP) to transmit data, as well as perform security related tasks) (Sperry, column 8, lines 6-24).

e. Locating the at least one security association using the information (obtaining security association data from the database) (Sperry, column 8, line 66-column 9, line 3).

f. Encrypting, decrypting or authenticating packets using the security association information (security arrangement has the capability of encryption, decryption and/or authentication of received data) (Sperry, column 4, lines 51-67).

As to claim 29, Sperry teaches the information comprises at least one address of the at least one security association (security association pointers are extracted to find the appropriate security association for that packet) (Sperry, column 8, line 66-column 9, line 3).

As to claim 30, Sperry teaches the at least one security processor generates an IPSec header using the information (generating and updating SAs for packets) (Sperry, column 11, line 29-column 12, line 56).

As to claim 31, Sperry teaches the at least one media access controller derives the information from context information associated with the TCP operations (Security Association pointers are extracted to find the appropriate security association for that packet) (Sperry, column 8, line 66-column 9, line 3).

As to claim 32, Sperry the at least one security processor is an integrated circuit and the at least one media access controller is an integrated circuit (Sperry, column 6, lines 35-37).

As to claim 33, the limitations of the claim have been addressed in claims 28 and 31 and are similarly rejected.

As to claim 41, the limitations of the claim have been addressed in claims 1 and 5 and are similarly rejected.

As to claims 46 and 55, Sperry teaches the at least one processor hashes at least a portion of the received data to extract at least one address of the security association information (use of the HMAC-SHA1 algorithm used for data flow encryption) (Sperry, column 8, lines 25-45).

As to claim 47, Sperry teaches:

a. At least one network controller (network processor) (Sperry, column 8, lines 47-55).

b. At least one cryptographic processor (Sperry, column 8, lines 25-46).

c. At least one MAC (Sperry, column 8, lines 25-46).

As to claim 48, Sperry teaches the at least one network controller adds information associated with at least one security association to at least a portion of the packets sent to the at least one security processor (security header encapsulation) (Sperry, column 8, lines 47-55).

As to claim 54, Sperry teaches locating at least one security association according to a security parameter index contained in at least one packet received from the at least one network (pointers) (Sperry, column 8, line 47-column 9, line 3).

As to claim 56, Sperry teaches at least one network controller securely communicates with the at least one security processor to configure the at least one security processor (flexible configuration of the security processor) (Sperry, column 8, lines 7-65).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

13. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

14. Claims 11, 49 and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,162,630 to Sperry et al. (hereinafter Sperry) as applied to claim 8 above, and further in view of US Patent No. 6,839,346 to Kametani.

As to claim 11, Sperry teaches a packet header (Sperry, column 5, lines 43-50) and information associated with a security association contained in a packet (SPI) (the Security Protocol Index (SPI) of an inbound packet is used to access the Protocol Control Block and the Security Association of the packet, if one exists) (Sperry, column 9, lines 4-20), but does not expressly mention that the security association information is contained in and extracted from the packet header. However, in an analogous art, Kametani teaches at least one processor for processing at least one frame header from the received data to extract security association information (extracting the SPI from the packet header to access the security association associated with that packet) (Kametani, column 13, lines 33-40).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the IPSec scheme of Sperry with the security association data embedded in the packet header of Kametani in order to obtain encryption information relating to the packet from the security association database as suggested by Kametani (Kametani, column 13, lines 38-40).

As to claim 49, Sperry as modified teaches adding at least one security header and trailer to at least a portion of the packets sent to the at least one security processor (Kametani, column 11, lines 43-53 and figure 7).

As to claim 50, Sperry as modified teaches modifying as least a portion of the at least one security header and trailer (refreshing of keying material) (Sperry, column 10, lines 49-57).

15. Claims 16-18 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,162,630 to Sperry et al. (hereinafter Sperry) in view of US Patent No. 6,157,955 to Narad et al. (hereinafter Narad).

As to claim 16, Sperry teaches

a. At least one Gigabit MAC (Sperry, column 8, lines 25-32).

b. At least one processor, connected to send data to and receive data from the at least one Gigabit MAC, for encrypting, decrypting or authenticating at least a portion of the data (the use of Network Protocol Processors (NPP) and Embedded Processors (EP) to transmit data, as well as perform security related tasks) (Sperry, column 8, lines 6-24).

Sperry does not expressly mention using a plurality of MACs in the security processor. However, in an analogous art, Narad teaches a plurality of MACs (Narad, column 7, line 63-column 8, line 9).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the IPSec scheme of Sperry with the multiple MACs of Narad in order to "accelerate network infrastructure applications" as suggested by Narad (Narad, column 1, lines 5-10).

As to claim 17, Sperry as modified teaches at least one processor comprises at least one IPSec processor (security processing is conformant to IPSec) (Sperry, column 5, lines 30-34).

As to claim 18, Sperry as modified teaches the IPSec processor adds IPSec protocol elements to or removes IPSec protocol elements from the data (security is added to packets that have security associations that require the packet to have security protocols) (Sperry, column 14, line 64-column 15, line 2).

As to claim 20, Sperry as modified teaches at least one data memory for storing security association information for use by the at least one processor (accessing security association data in order to properly handle data packets) (Sperry, column 12, line 65-column 13, line 15).

16. Claims 19 and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,162,630 to Sperry et al. (hereinafter Sperry) in view of US Patent No. 6,157,955 to Narad et al. (hereinafter Narad) as applied to claim 16 above, and further in view of US Patent No. 6,839,346 to Kametani.

As to claim 19, Sperry as modified teaches a packet header (Sperry, column 5, lines 43-50) and information associated with a security association contained in a packet (SPI) (the Security Protocol Index (SPI) of an inbound packet is used to access the Protocol Control Block and the Security Association of the packet, if one exists) (Sperry, column 9, lines 4-20), but does not expressly mention that the security association information is contained in and extracted from the packet header. However, in an analogous art, Kametani teaches at least one processor for processing at least one frame header from the received data to extract security association information (extracting the SPI from the packet header to access the security association associated with that packet) (Kametani, column 13, lines 33-40).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the IPSec scheme of Sperry with the security association data embedded in the packet header of Kametani in order to obtain encryption information relating to the packet from the security association database as suggested by Kametani (Kametani, column 13, lines 38-40).

As to claim 51, Sperry as modified teaches modifying at least one checksum in the at least one security header added by the at least one network controller (updating checksum of the packet) (Narad, column 115, lines 7-22).

17. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,162,630 to Sperry et al. (hereinafter Sperry) as applied to claim 21 above, and further in view of US Patent No. 7,062,566 to Amara et al. (hereinafter Amara).

As to claim 24, Sperry does not expressly mention the use of VLAN tags. However, in an analogous art, Amara teaches the at least one switch associates VLAN tags with the at least one media access controller (VLAN tags are used as packet identifiers) (Amara, column 4, lines 12-36).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the IPSec scheme of Sperry with the VLAN tags of Amara in order to obtain the correct IPSec policies and apply them to the packet as suggested by Amara (Amara, column 4, lines 30-36).

18. Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,162,630 to Sperry et al. (hereinafter Sperry) in view of US Patent No. 6,959,007 to Vogel et al. (hereinafter Vogel).

As to claim 27, Sperry teaches:

a. At least one media access controller (Sperry, column 8, lines 25-32).

b. At least one security processor (the use of Network Protocol Processors (NPP) and Embedded Processors (EP) to transmit data, as well as perform security related tasks) (Sperry, column 8, lines 6-24).

c. At least one switch for routing packets between the at least one media access controller and the at least one security processor (the use of switches in the target environment) (Sperry, column 7, lines 5-19).

Sperry does suggest differing circuit layouts (Sperry, column 6, lines 35-48), but does not expressly use the terms backplane and blade in defining the architecture of the security processor. However, in an analogous art, Vogel teaches:

d. At least one backplane (Vogel, column 5, lines 17-33).

e. At least one processing blade connected to the at least one backplane (Vogel, column 5, lines 17-33).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the IPSec scheme of Sperry with the backplane and blade configuration of Vogel in order to achieve an architecture that is cheaper, requires a lower chip count, requires less power and provide adequate bandwidth as suggested by Vogel (Vogel, column 1, lines 48-52).

19. Claims 40, 52 and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,162,630 to Sperry et al. (hereinafter Sperry) in view of US Patent No. 6,947,430 to Bilic et al. (hereinafter Bilic).

As to claim 40, Sperry teaches using TCP packets (Sperry, column 5, lines 1-23), the use of headers in the packets that contain information about security associations

(Sperry, column 5, lines 43-50) and creating security associations for packets (Sperry, column 11, lines 31-60) but does not expressly mention appending the header to a packet. However, in an analogous art, Bilic teaches:

a. Generating an Ethernet header (Bilic, column 7, lines 57-62).

b. Appending the at least one header to an original TCP frame (generating a complete packet by merging header and payload) (Bilic, column 8, lines 26-32).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the IPSec scheme of Sperry with the header generation and merging of Bilic in order to achieve high-speed packet header processing as suggested by Bilic (Bilic, column 1, lines 12-15).

As to claims 52 and 53, Sperry as modified teaches modifying at least one maximum transmitted unit size in accordance with modifications the security processor makes to at least a portion of the packets (there is a maximum packet size and the size of the payload is in direct proportion to the size of the at least one header) (Bilic, column 8, lines 10-37).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to William S. Powers whose telephone number is 751 272 8573. The examiner can normally be reached on m-f 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

William S. Powers
Examiner
Art Unit 2134

5/8/2007